No.

In the Supreme Court of the United States

ROSS WILLIAM ULBRICHT, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

KANNON K. SHANMUGAM
Counsel of Record
ALLISON JONES RUSHING
MASHA G. HANSFORD
MICHAEL J. MESTITZ
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
(202) 434-5000
kshanmugam@wc.com

QUESTIONS PRESENTED

1. Whether the warrantless seizure of an individual's Internet traffic information without probable cause violates the Fourth Amendment.

2. Whether the Sixth Amendment permits judges to find the facts necessary to support an otherwise unreasonable sentence.

TABLE OF CONTENTS

Page

Table of contents—continued:

TABLE OF AUTHORITIES

Cases:

Page

Cases—continued:

Constitution and statutes:

Page

In the Supreme Court of the United States

No.

ROSS WILLIAM ULBRICHT, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

Ross William Ulbricht respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Second Circuit in this case.

OPINIONS BELOW

The opinion of the court of appeals (App., *infra*, 3a-108a) is reported at 858 F.3d 71. The district court's order denying petitioner's motion to suppress (App., *infra*, 109a-146a) is unreported.

JURISDICTION

The judgment of the court of appeals was entered on May 31, 2017. A petition for rehearing was denied on August 30, 2017. On November 21, 2017, Justice Ginsburg extended the time within which to file a petition for a writ of certiorari to and including December 28, 2017. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

CONSTITUTIONAL PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution provides in relevant part:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause[.]

The Sixth Amendment to the United States Constitution provides in relevant part:

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury[.]

STATEMENT

This case—one of the highest-profile federal criminal prosecutions in recent years—presents two important questions requiring the Court's review. The first question is whether the warrantless seizure of an individual's Internet traffic information without probable cause violates the Fourth Amendment. That question is closely related to the question the Court is currently considering in *Carpenter* v. *United States*, cert. granted, No. 16-402 (argued Nov. 29, 2017). The second question is whether the Sixth Amendment forbids a judge from finding facts necessary to support an otherwise unreasonable sentence. The Court left open that question a decade ago in *Rita* v.

United States, 551 U.S. 338 (2007). As to both questions, the courts of appeals have expressed serious doubts about the constitutionality of existing practices, but they perceive themselves to be bound by the Court's precedents.

In this case, without a warrant or probable cause, the government seized petitioner's private Internet traffic information and used that information to arrest and convict him of drug trafficking and related offenses. The district court then sentenced petitioner to life imprisonment without the possibility of parole—a sentence almost unheard of for a first-time offender charged with the offenses at issue. The district court imposed that sentence by resolving several disputed issues of fact; absent those judge-found facts, petitioner's sentence would have been unreasonable.

The court of appeals affirmed. Although the court acknowledged that "questions have been raised" about the constitutionality of both practices, it considered itself bound to apply this Court's precedents on those issues "until and unless" the Court intervenes. App., *infra*, 33a; see *id.* at 106a n.72. This case is an appropriate vehicle in which to provide much-needed clarity on critical and recurring questions of federal criminal law.

1. In 2009, petitioner, a 25-year-old committed libertarian with a master's degree in materials science and engineering, began working to create an online marketplace that would allow users to buy goods anonymously and securely. Petitioner's efforts culminated in 2011 in the creation of a website called the Silk Road, which allowed individual users to create anonymous accounts to buy and sell a range of goods and services. As petitioner later told the district court: "I remember clearly why I created the Silk Road. I had a desire to—I wanted to empower people to be able to make choices in their lives for themselves and to have privacy and anonymity." C.A. App. 1507. Users

bought and sold a variety of illegal goods on the Silk Road website, including drugs, false identification documents, and computer hacking software. App., *infra*, 5a.

In 2012, the lead administrator of the Silk Road adopted the username "Dread Pirate Roberts," a reference to the novel and film *The Princess Bride* (in which Dread Pirate Roberts was a pseudonym periodically passed from one individual to another). Petitioner contended at trial that he abandoned his interest in the Silk Road in 2011, but was lured back by a successor administrator toward the end of the site's operation so that he would take the blame for the site. App., *infra*, 14a, 19a.

2. The government began investigating the Silk Road website in 2011 after it started to receive attention in the news media. The government initially targeted "several individuals" it suspected of being the Dread Pirate Roberts, including Mark Karpeles, a computer developer and a self-proclaimed hacker. According to the government, it began to focus on petitioner when it found an Internet post on one of Karpeles' websites relating to the Silk Road. The post was made by a user associated with the e-mail address rossulbricht@gmail.com. App., *infra*, 6a; Gov't C.A. Br. 64-65; Tr. 1263, 1266-1267 (Jan. 26, 2015).

Using that e-mail address, the government was able to locate petitioner and eventually to monitor his Internet traffic and location. To begin with, the government identified a particular Internet Protocol (IP) address that regularly accessed petitioner's e-mail account. An IP address is a unique number assigned to every device connected to the Internet. When a user visits a webpage, checks his e-mail, or performs any other action requiring an Internet connection, his computer or device communicates its IP address so the responding computer knows how to route the requested data. App., *infra*, 7a.

The government collected data about the Internet traffic to and from petitioner's IP address and identified his home address as 235 Monterey Boulevard in San Francisco, California. The government then secured an order authorizing a "pen register," along with a "trap and trace device," to be applied to the wireless router in petitioner's living room. A pen register is a device that records the dialing, routing, addressing, or signaling information transmitted by a particular device, such as a telephone, computer, or e-mail account. App., *infra*, 30a, 112a-114a; Gov't C.A. Br. 105-106.

In order to obtain an order authorizing a pen register under Title III of the Electronic Communications Privacy Act, the government is not required to show probable cause; instead, a government attorney need only certify that the information "likely to be obtained" by the pen register is "relevant" to an ongoing criminal investigation. 18 U.S.C. 3122. A trap and trace device is like a pen register, only it collects incoming (rather than outgoing) data. Together, the combination of a pen register and a trap and trace device is known as a "pen/trap."

The orders authorizing the pen/trap on the router in petitioner's home, like other pen/traps the government later employed, allowed the government to collect several categories of information associated with petitioner's Internet activity. Specifically, orders allowed the government to "identify the source and destination IP addresses, along with the dates, times, durations, ports of transmissions, and any Transmission Control Protocol (TCP) connection data[] associated with any electronic communication sent to or from" specified devices associated with petitioner, including his router and laptop. App., *infra*, 30a-31a (alteration, footnote, and citation omitted).

The pen/trap orders allowed the government to determine the IP addresses contacted by petitioner's router;

the time and duration of those connections; and the individual devices that were connecting to the Internet through the router. By identifying the "port of transmission" associated with petitioner's Internet traffic, the pen/trap orders also allowed the government to determine what *type* of Internet traffic was occurring. As the government's lead FBI investigator explained: "Computers use different 'ports' to handle different types of Internet traffic. For example, e-mail traffic is handled on certain ports while website traffic is handled on others. Port information thus reveals what type of traffic is reflected on a pen register[.]" D. Ct. Dkt. 57, at 9 (¶ 19 n.10) (Sept. 5, 2014) (declaration of Christopher Tarbell).

As a result of the pen/trap orders, the government was able to identify all of the individual devices that regularly connected with petitioner's router, along with the traffic associated with those devices. In particular, the government determined that a particular laptop computer—petitioner's personal laptop—routinely connected with the router. The government did so by identifying the media access control (MAC) address of the laptop—a unique number embedded in a device's hardware that can be used to identify the device on any network to which it connects. After identifying the MAC address of petitioner's laptop, the government could isolate the Internet traffic associated with that computer. App., *infra*, 30a-31a; D. Ct. Dkt. 57, at 9 (¶ 19 n.11).

Using that MAC address, the government secured yet another pen/trap order to collect data about any Internet communications sent to or from petitioner's laptop. During this period, the government monitored petitioner's Internet activity, including the times he logged on and off, to compare it with the Dread Pirate Roberts' Internet activity. After two weeks of warrantless pen/trap surveillance, agents sought a warrant for petitioner's arrest, as

well as warrants to search his home and laptop. Petitioner was subsequently arrested at a public library in San Francisco. App., *infra*, 12a, 112a-114a; Gov't C.A. Br. 107-108.

3. A grand jury in the Southern District of New York indicted petitioner on numerous counts of drug trafficking and related offenses. Before trial, petitioner moved to suppress evidence gathered in the course of the government's warrantless pen/trap surveillance, contending that the pen/trap orders were unlawful because a warrant was required. App., *infra*, 7a-8a, 31a.

The district court denied the motion. App., *infra*, 110a, 141a-142a. The court relied on this Court's decision in *Smith* v. *Maryland*, 442 U.S. 735 (1979), which held that individuals have no Fourth Amendment privacy interest in phone numbers captured during a telephone call by a pen register. App., *infra*, 141a-142a. Based on that holding, the district court concluded that the "law is clear—and there is truly no room for debate—that the type of information" gathered by the pen/trap orders at issue here "was entirely appropriate for that type of order." App., *infra*, 141a.[1]

4. After a highly publicized trial, petitioner was convicted on all counts. Under the relevant statutes, petitioner's convictions exposed him to a mandatory minimum sentence of 240 months in prison and a maximum sentence of life in prison. Under the Sentencing Guidelines, petitioner's offenses and complete lack of criminal history should have led to a recommended Guidelines range substantially below that maximum.

---

[1] Although the district court also determined that petitioner had not demonstrated he possessed a sufficient interest in the information at issue, App., *infra*, 141a-142a & n.14, the government stipulated that petitioner had such an interest, and the court of appeals proceeded to address the constitutionality of the pen/trap orders, *id.* at 31a n.28.

At petitioner's sentencing hearing, however, the district court resolved several disputed issues of fact by a preponderance of the evidence and applied several enhancements to petitioner's offense level. The court imposed an increase for directing the use of violence, based on its determination that petitioner commissioned five murders (which were never committed) during his alleged time as the Dread Pirate Roberts. Petitioner was not charged for the alleged commissioning of murders; indeed, at trial, the government did not claim the murders actually occurred and stressed to the jury that it was "not required to make any findings about them." Tr. 2159-2160 (Feb. 3, 2015). But the district court discussed the alleged commissioning of murders at length at sentencing and imposed an enhancement on that basis. App., *infra*, 26a-27a; C.A. App. 1464-1466, 1528-1529.

The district court also made findings resulting in an increase under the Guidelines for importing methamphetamine; an increase for maintaining premises for manufacturing or distributing a controlled substance; and an increase for distributing a drug quantity far in excess of the quantity found by the jury. Because the offense level resulting from these enhancements exceeded the maximum allowable level, the Guidelines "range" became a recommended sentence of life imprisonment. App., *infra*, 26a-27a; C.A. App. 1463-1470.

The district court also devoted extensive attention at sentencing to other conduct for which petitioner was never charged. In particular, the district court considered evidence of six drug-related deaths allegedly connected to Silk Road, including testimony from parents of two of the decedents. App., *infra*, 27a-28a; C.A. App. 1472-1496. Although the court noted that "[t]he defendant is not convicted of killing these people" and the evidence of the deaths was "not relevant to the offenses of conviction," it

determined it could consider the deaths as "related conduct" on the theory that they were, "by a preponderance of the evidence * * * , in some way, related to the Silk Road." C.A. App. 1472.

The defense objected to the district court's factual findings. C.A. App. 1481. Petitioner also submitted almost one hundred letters attesting to his character, which the court called "profoundly moving," "written by a vast, broad array of people * * * from every phase of your life," and which showed "a man who was loved, who has built enduring and significant relationships over a lifetime and maintained them, * * * [who] displayed great kindness to many people." *Id.* at 1534-1535. The government's sentencing letter to the court nevertheless urged a "lengthy sentence," citing the fact that petitioner's "sentencing [was] being closely watched." *Id.* at 1328.

Noting the "significant public interest in this case," the district court sentenced petitioner (who was then 31 years old) to life imprisonment. The court also imposed a forfeiture order of $184 million, representing the amount that allegedly passed through the Silk Road website. C.A. App. 1537-1539.

5. On appeal, petitioner argued, as is relevant here, that the district court erred in denying his motion to suppress the evidence from the pen/trap orders and that his life sentence was both procedurally and substantively unreasonable.

The court of appeals affirmed. App., *infra*, 3a-108a. As to the denial of petitioner's motion to suppress, the court adopted the government's assertion that the collected information about Internet traffic was "akin to data captured by traditional telephonic pen registers and trap and trace devices." *Id.* at 31a (internal quotation marks and citation omitted). Relying on the so-called "third-party doctrine" developed in the context of telephone calls

in *Smith*, the court concluded that petitioner had no reasonable expectation of privacy in his Internet traffic information because he voluntarily conveyed it to his Internet service provider and to third-party servers. *Id.* at 32a-33a. Although the court acknowledged that "questions have been raised about whether some aspects of modern technology * * * call for a re-evaluation" of the rule of *Smith*, it nevertheless viewed itself as "bound * * * by [*Smith*] until and unless it is overruled by the Supreme Court." *Id.* at 33a.

As to the reasonableness of the sentence, the court of appeals ultimately upheld the sentence, although it did "not reach [its] conclusion lightly." App., *infra*, 107a. Even though a "life sentence for selling drugs alone would give pause," the court of appeals differentiated this case from the typical drug-trafficking case based on the district court's factual findings at sentencing. *Id.* at 100a-101a. In particular, the court reasoned that the district court's finding that petitioner had "[c]ommission[ed] * * * murders significantly justified the life sentence," rendering it substantively reasonable. *Id.* at 101a n.68; see *id.* at 102a.

The court of appeals likewise upheld petitioner's sentence as procedurally reasonable, despite the district court's decision to take into account the drug-related deaths. App., *infra*, 87a-97a. At the outset, the court of appeals stated that there was "no need" for the government to introduce such "emotionally inflammatory" evidence at sentencing, "let alone to hammer the point home with unavoidably emotional victim impact statements by parents of two of the decedents." *Id.* at 91a. But the court of appeals ultimately concluded that the district court was permitted to consider the uncharged conduct, found by a

preponderance of evidence, as long as the facts did not increase the statutory maximum sentence for the crimes for which petitioner was found guilty. *Id.* at 92a-93a, 96a.

Petitioner and his amici cited various opinions by members of this Court suggesting that judicial factfinding violates a defendant's constitutional right to a jury trial where it renders reasonable an otherwise unreasonable sentence. Pet. C.A. Reply Br. 60-62; see, *e.g.*, Drug Policy Alliance C.A. Br. 14-15. But the court of appeals rejected petitioner's constitutional argument as having "no support in existing law." App., *infra*, 106a n.72. Although the court of appeals "might not have imposed the same sentence [itself] in the first instance" in this case, it determined that the district court's factual findings brought petitioner's sentence within a permissible range. *Id.* at 107a. Based on those findings, the court of appeals upheld what it described as the district court's exercise of its "power to condemn a young man to die in prison." *Id.* at 108a.

6. The court of appeals denied a petition for rehearing without recorded dissent. App., *infra*, 1a-2a.

REASONS FOR GRANTING THE PETITION

I. THIS COURT SHOULD GRANT REVIEW TO DECIDE WHETHER THE FOURTH AMENDMENT PROTECTS AN INDIVIDUAL'S INTERNET TRAFFIC INFORMATION

A. The Question Presented Is Of Exceptional Importance And Cannot Be Answered Without This Court's Review

This case presents the question whether the Fourth Amendment permits the government, without probable cause, to collect data generated by millions of individuals as an everyday incident of modern life: their Internet traffic information. The Court has previously granted certiorari to resolve similar questions about the interplay

between modern technology and Fourth Amendment privacy interests, see, *e.g.*, *Riley* v. *California*, 134 S. Ct. 2473 (2014), and it has done so again this Term, see, *e.g.*, *Carpenter* v. *United States*, cert. granted, No. 16-402 (argued Nov. 29, 2017). The Court should similarly grant certiorari to resolve the question presented in this case or, at a minimum, hold this case pending its decision in *Carpenter*, which may articulate principles applicable here.

1. Courts of appeals addressing the question presented here have largely felt constrained by this Court's ill-fitting precedents from a generation ago concerning privacy interests in dialed telephone numbers revealed to, and physical papers held by, third parties. At the same time, the courts of appeals have signaled the need for this Court to address whether, and how, those precedents apply in the context of modern Internet technology.

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. In *Smith* v. *Maryland*, 442 U.S. 735 (1979), this Court held that the Fourth Amendment did not forbid law enforcement from using a pen register to capture telephone numbers dialed by individual telephone users. See *id.* at 745-746. The Court reasoned that an individual's expectation of privacy in the numbers he dialed was diminished because the individual "voluntarily conveyed" that information to the phone company. *Id.* at 744 (citation omitted). The Court doubted that "people in general entertain any actual expectation of privacy in the numbers they dial," observing that an individual would have known that the phone company recorded those numbers because they would be listed on the individual's bills. *Id.* at 742. In reaching its decision, the Court emphasized the pen register's "limited capabilities," noting that "a law enforcement official could not even determine from the

use of a pen register whether a communication existed" or "whether the call was even completed." *Id.* at 741-742 (citation omitted). Similarly, in *United States* v. *Miller*, 425 U.S. 435 (1976), the Court relied in part on the notion of voluntary conveyance in holding that a bank customer lacked a Fourth Amendment privacy interest in papers held by a bank. See *id.* at 442-443.

Courts of appeals, including the court of appeals below, have applied *Smith* and *Miller* to reject individuals' Fourth Amendment privacy interests in their Internet traffic information, even while calling on this Court for guidance on the question. In the decision below, for example, the court of appeals considered itself "bound" by *Smith* "until and unless it is overruled by the Supreme Court." App., *infra*, 33a. Similarly, the Seventh Circuit has noted that, although "at least one Justice believes 'it may be necessary' to reconsider the third-party doctrine * * *, [u]ntil the Court says otherwise, [*Smith* and *Miller*] bind us." *United States* v. *Caira*, 833 F.3d 803, 809 (7th Cir. 2016) (citation omitted), petition for cert. pending, No. 16-6761 (filed Nov. 7, 2016).

The Third Circuit, in particular, has flagged the conundrum facing the lower courts. In *United States* v. *Stanley*, 753 F.3d 114, cert. denied, 135 S. Ct. 507 (2014), the defendant surreptitiously connected his computer to his neighbor's wireless router and used his neighbor's network to download child pornography. Although the Third Circuit held that the defendant could not claim any legitimate expectation of privacy in the information he transmitted while "wrongful[ly]" connected to his neighbor's wireless network, it cautioned that the district court "went too far" in relying on *Smith* categorically to reject any privacy interest in the defendant's wireless signal. *Stanley*, 753 F.3d at 120-123. The court reasoned that such an approach would "open a veritable Pandora's Box

of Internet-related privacy concerns," because "[t]he Internet, by its very nature, requires *all* users to transmit their signals to third parties." *Id.* at 124.

To be sure, some courts have considered the question presented to be "constitutionally indistinguishable from [the question in] *Smith*," *United States* v. *Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), despite this Court's admonition in a similar context that "any extension" of analogera reasoning to digital data "has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489; see, *e.g.*, *United States* v. *Christie*, 624 F.3d 558, 573-574 (3d Cir. 2010), cert. denied, 562 U.S. 1236 (2011); *United States* v. *Bynum*, 604 F.3d 161, 164 (4th Cir.), cert. denied, 560 U.S. 977 (2010). But those decisions only underscore the necessity of this Court's intervention. Calling the Internet traffic information collected by pen/traps today "constitutionally indistinguishable" from the list of telephone numbers at issue in *Smith* is "like saying a ride on horseback is materially indistinguishable from a flight to the moon": "[b]oth are ways of getting from point A to point B, but little else justifies lumping them together." *Riley*, 134 S. Ct. at 2488. The Court should address the question presented and provide lower courts with guidance pertinent to the application of Fourth Amendment principles to modern Internet technology.

2. This Term, the Court is already considering a closely related question in *Carpenter*: namely, whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user is permitted by the Fourth Amendment. See Pet. at i, *Carpenter*, *supra*. This case presents an ideal opportunity for the Court to resolve a similar legal question concerning Internet traffic information in tandem with the question presented in *Carpenter*. Both *Carpenter* and this case turn on whether lower courts are correct

in applying the rationale of *Smith* and *Miller* to certain types of data transmitted to third parties. Indeed, in the decision below in this case, the court of appeals cited the Sixth Circuit's decision in *Carpenter* for the proposition that courts have not extended Fourth Amendment protection to information concerning IP addresses. App., *infra*, 34a.

This case is an appropriate companion case to *Carpenter* because the Internet traffic information at issue here is broader in important ways than the cell site location information at issue in *Carpenter*. In addition to allowing the government to determine when petitioner was accessing the Internet from the privacy of his own home, the information gathered by the pen/traps here permitted the government to determine the websites to which petitioner connected, the length of the connections, and the port of transmission of the data. As this Court has recognized, the collection of such Internet information could reveal "an individual's private interests or concerns." *Riley*, 134 S. Ct. at 2490.

Accordingly, a decision in the government's favor in *Carpenter* is unlikely to resolve the question presented here, because *Carpenter* provides no opportunity for the Court to rule on Internet traffic information (such as information concerning IP addresses and ports of transmission). The Court's decision in *Carpenter* thus may leave the lower courts without the specific guidance they need. Such a piecemeal approach would deprive law enforcement of "clear rules" regarding such data, and "it would take many cases and many years" for the federal courts of appeals to reevaluate and adjust their approach to Internet traffic information. *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring in part and concurring in judgment). In that time, "the nature of the electronic devices" possessed

by "ordinary Americans * * * would continue to change." *Ibid.*

It would be most efficient for the Court to resolve the question presented in this case now, while it is considering a related question in *Carpenter*. Such an approach would enable the Court's decision in each case to be informed by the potential implications presented by the other.

3. At a minimum, the Court should hold this petition pending its decision in *Carpenter*. Notably, the Court appears to be holding another petition presenting a similar question concerning the Fourth Amendment interest in IP address information. See *United States* v. *Caira*, *supra* (No. 16-6761). In *Caira*, the government identified alleged criminal activity associated with a particular Hotmail address and issued an administrative subpoena to Microsoft, which owns the Hotmail domain. See 833 F.3d at 805. In response, Microsoft disclosed a list of IP addresses used to access the e-mail account. See *ibid.* Identifying one of the IP addresses, the government issued a second administrative subpoena to Comcast to identify the physical address associated with that IP address. See *ibid.* The defendant moved to suppress the evidence, arguing that he possessed a Fourth Amendment privacy interest in information concerning IP addresses, but the Seventh Circuit rejected the defendant's claim by invoking *Smith* and *Miller*. See *id.* at 806-807.

In light of the Court's apparent conclusion that *Caira* presents a similar enough question for that petition to be held pending *Carpenter*, this petition should at a minimum also be held. Both this case and *Caira* turn on whether information that may be collected incident to an individual's Internet browsing activity, including information concerning IP addresses, is entitled to Fourth Amendment protection. And both courts of appeals relied centrally on *Smith* and *Miller* in rejecting the defendants'

arguments. If the Court does not grant certiorari outright in this case, therefore, it should at least hold the petition pending the resolution of *Carpenter*.

B. The Decision Below Is Erroneous

***1. Internet Traffic Information Is Not Analogous To The Telephone Routing Information Gathered In* Smith *v.* Maryland**

In upholding the warrantless seizure at issue here, the court of appeals explained that collecting Internet traffic information (such as information concerning IP addresses and ports of transmission) was "precisely analogous to the capture of telephone numbers at issue in *Smith*." App., *infra*, 33a. But *Smith* is distinguishable from this case in important respects and should not be extended to Internet traffic information. In *Smith*, the pen register that was applied to the defendant's telephone had only "limited capabilities": it could not tell the government "the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed." 442 U.S. at 741-742 (citation omitted). Here, by contrast, the pen/traps allowed the government to "identify the source and destination IP addresses, along with the dates, times, durations, ports of transmission, and any Transmission Control Protocol ('TCP') connection data, associated with any electronic communications sent to or from" petitioner's devices, including his laptop and his wireless router. App., *infra*, 30a-31a (alteration, footnote, and citation omitted). Each of these categories of data is significant individually; collectively, they far exceed the data collected by the pen register at issue in *Smith*.

a. To begin with, unlike in *Smith*, the government could identify the "purport of any communication" at issue

here, because it collected the ports of transmission of petitioner's Internet activity. A "port" is a piece of information used to identify the purpose of a particular packet of data being transmitted between computers. D. Ct. Dkt. 57, at 9 (¶ 19 n.10); see PC Magazine, *Definition of TCP/IP Port* <tinyurl.com/portdefinition> (last visited Dec. 22, 2017). For example, if port numbers "80" or "443" appeared in connection with petitioner's Internet activity, the government would know that petitioner was accessing a webpage. Similarly, if port numbers "25," "110," or "143" appeared, the government would know that petitioner was using an e-mail application.

b. More broadly, an individual's Internet traffic information is far more sensitive than the telephone routing information at issue in *Smith*. As this Court has observed, "[a]n Internet search and browsing history * * * [can] reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD." *Riley*, 134 S. Ct. at 2490. Extending *Smith* and *Miller* to Internet traffic information would allow the government to access significant information about an individual's Internet habits without a warrant and without probable cause. For example, the government could learn that the individual regularly visits websites associated with a particular political party or sexual orientation, "enabl[ing] the Government to ascertain, more or less at will, [people's] political and religious beliefs, sexual habits, and so on." *United States* v. *Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

Individuals today use the Internet to apply for jobs, find love, answer questions, keep up with news and politics, and engage with one another on "websites integral to the fabric of our modern society and culture." *Packingham* v. *North Carolina*, 137 S. Ct. 1730, 1738 (2017). Some 90% of U.S. adults today use the Internet, and 77% report

that they use it either "several times a day" or "almost constantly." Pew Research Center, *Tech Adoption Climbs Among Older Adults* 7, 21 (May 17, 2017) <tinyurl.com/pewtechuse>.

In *Smith*, the government could not even determine whether a connection was completed. 442 U.S. at 741. Here, by contrast, the government's data not only showed whether a connection "was * * * completed," *ibid.*, but also for how long the connection lasted—far more detail than the pen register provided in *Smith*.

What is more, pen/traps revealing IP address information can also allow the government to identify an individual's general location, as the government demonstrated at petitioner's trial. See Tr. 102-103, 105-106 (Jan. 13, 2015). In addition, by placing pen/traps on petitioner's laptop and wireless router, the government could determine when petitioner was using his laptop in his home by monitoring when petitioner's laptop was connected to the Internet.

In that respect, the government turned petitioner's laptop into an analogue of the tracking device at issue in *United States* v. *Karo*, 468 U.S. 705 (1984). In that case, the Court held that the government conducted an unconstitutional search when it monitored a signal from a tracking device in the defendant's home without a warrant. *Id.* at 718. The Court observed that, even when a digital tracking device is accompanied by conventional surveillance, it implicates the Fourth Amendment because it confirms for the government that "a particular article is actually located at a particular time in the private residence" and that the article "remains on the premises"—information that the government "could not have otherwise obtained without a warrant." *Id.* at 715. Here, as in *Karo*, the government should not be "free * * * to determine by means of an electronic device, without a warrant and

without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time." *Id.* at 716.

The significant breadth and sensitivity of Internet traffic information distinguishes this case from *Smith* and counsels in favor of Fourth Amendment protection. Extending *Smith* and *Miller* to Internet traffic information "entrust[s] to the Executive" tremendous power that is "amenable to misuse" and runs counter to "the Fourth Amendment's goal to curb arbitrary exercises of police power and prevent 'a too permeating police surveillance.'" *Jones*, 565 U.S. at 416-417 (Sotomayor, J., concurring) (quoting *United States* v. *Di Re*, 332 U.S. 581, 595 (1948)). When agents can gather an individual's Internet traffic information upon only the minimal showing required by the Electronic Communications Privacy Act, little beyond their discretion constrains their ability to monitor citizens' private lives. And an agent's choice to exercise discretion is no substitute for clear limits imposed by an impartial magistrate. See *Katz* v. *United States*, 389 U.S. 347, 356-357 (1967).

c. In many cases, moreover, Internet traffic information is not shared voluntarily, because computers and other devices often connect to the Internet without requiring a user to act. Applications on those devices automatically connect to Internet servers and check for updates, fetch e-mail, or send data without users' knowledge. That information can be valuable—for example, to establish that an individual has certain software installed on his computer. But it cannot be said to have been "voluntarily conveyed" to a third party. *Smith*, 442 U.S. at 744.

Even when a user voluntarily acts to enter an Internet address into his browser, the "voluntary" disclosure of that information is unlike the disclosure in *Smith*. There,

the Court reasoned, telephone customers knew that companies recorded the numbers they dialed because telephone customers could "see a list of their long-distance (toll) calls on their monthly bills." 442 U.S. at 742. Internet service providers, by contrast, do not provide that information to their customers, nor do they routinely share information about ports of transmission.

2. Individuals Have A Reasonable Expectation Of Privacy In Their Internet Traffic Information

The court of appeals applied *Smith* and *Miller* to hold that conveying Internet traffic information to a third party destroyed any privacy interest in that information. But there is no reason to extend those decisions to the information at issue in this case. Internet users may not even understand that they are providing that sensitive and revealing information, much less that they are relinquishing any expectation of privacy by conveying it. As this Court recently cautioned, reflexively relying on "pre-digital analogue[s]" risks "a significant diminution of privacy." *Riley*, 134 S. Ct. at 2493.

Individuals overwhelmingly consider their Internet browsing habits to be private. A 2014 Pew Research survey found that 70% of adults consider the websites they have visited to be "very sensitive" or "somewhat sensitive" information. Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* 37 (Nov. 12, 2014) <tinyurl.com/privacystudy>. As Justice Sotomayor has noted, it is "doubt[ful] that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year." *Jones*, 565 U.S. at 418 (concurring opinion). Yet that is precisely what can happen when the government places a pen/trap on individuals' computers.

This problem, moreover, is no longer limited merely to Internet traffic from desktop and laptop computers; it applies with equal force to any Internet-enabled device that connects to a wireless network. If petitioner's smartphone had been connected to his wireless network at home, the Internet traffic information from that phone would have traveled through his router and been captured by the government's pen/trap. To the extent that traffic associated with data sent to or from any of the many applications on a user's phone will be swept into the government's net, the court of appeals' holding implicates many of the concerns this Court has already addressed in *Riley*. See 134 S. Ct. at 2490 (describing "apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; [and] apps for improving your romantic life"). Indeed, the government can readily identify which applications an individual has on his phone from the destination IP addresses of the data transmitted from those applications.

It is not difficult to conclude that individuals have a reasonable expectation of privacy that is cognizable under the Fourth Amendment in the highly personal information that may be revealed by a pen/trap collecting Internet traffic information. The government should not be free to collect that information without the constraint of a warrant or any showing of probable cause.

C. The Question Presented Warrants Review In This Case

This case presents a timely opportunity to consider the question presented on a well-developed record.

1. This case presents the constitutional question in an ideal context for addressing the relationship between

Smith and modern technology. The Internet traffic information gathered in this case was significant both in quantity and quality. The pen/trap orders permitted the government prospectively to collect petitioner's Internet traffic information for 60 days. See Pet. C.A. Br. 110. Ultimately, the government collected gigabytes of data on petitioner's Internet activity over a matter of weeks, and swept in tens of thousands of individual transmissions, if not more.

The pen/trap on petitioner's laptop, in particular, allowed the government to identify when petitioner was connected to the Internet, which websites petitioner accessed during his browsing session, and for how long. That information was much more invasive than, for example, the information collected in *Caira*, which was limited to historical records of IP addresses that had accessed a particular e-mail account (along with the physical address associated with the defendant's IP address). See 833 F.3d at 805. And this case offers the Court an opportunity to address the question presented in the context of the Electronic Communications Privacy Act, the statute governing the issuance of orders authorizing pen registers and trap and trace devices.

2. The question presented was also preserved at each stage of the proceedings below. In the district court, petitioner argued that "the information obtained through the [pen/trap orders] should have been the subject of a warrant application," and he specifically argued that *Smith* did not apply. App., *infra*, 141a-142a & n.14. And the court of appeals, recognizing that petitioner "made the same arguments" in the district court, addressed the question presented at length, ultimately concluding that it was bound by *Smith* to reject petitioner's claims "until and unless it is overruled by the Supreme Court." *Id.* at 31a n.28, 33a. The question presented is thus ripe for the

Court's review in this case, and the Court's guidance on that question is sorely needed.

II. THIS COURT SHOULD GRANT REVIEW TO DECIDE WHETHER THE SIXTH AMENDMENT PERMITS A JUDGE TO FIND THE FACTS NECESSARY TO SUPPORT AN OTHERWISE UNREASONABLE SENTENCE

This case also presents the unrelated, but equally important, question whether the Sixth Amendment permits judges, as opposed to juries, to find facts necessary to render a sentence reasonable. This Court has repeatedly "left [that question] for another day." *Jones* v. *United States*, 135 S. Ct. 8, 8-9 (2014) (Scalia, J., dissenting from the denial of certiorari). And as in this case, the courts of appeals have interpreted the Court's silence as consent to the proposition that an otherwise unreasonable sentence supported by judicial factfinding is constitutional as long as it is within the statutory sentencing range—despite the contrary import of the Court's sentencing decisions.

"This has gone on long enough." *Jones*, 135 S. Ct. at 9 (Scalia, J., dissenting from the denial of certiorari). And it is hard to imagine a better example of the consequences of runaway judicial factfinding than this case. Petitioner, a young man with no criminal history, was sentenced to life imprisonment without the possibility of parole for drug crimes that do not ordinarily carry that sentence, based substantially on numerous factual findings made by the sentencing judge by a preponderance of the evidence. The Court should finally resolve this long-unsettled question and put an end to unconstitutional sentences such as petitioner's.

A. The Question Presented Is An Important One Expressly Reserved By This Court And Subject To Extensive Debate By Judges In The Lower Courts

1. In *Rita* v. *United States*, 551 U.S. 338 (2007), this Court held that applying a presumption of reasonableness to within-Guidelines sentences is constitutional on the ground that the Sixth Amendment does not "automatically forbid" a judge from taking account of factual matters not determined by the jury. *Id.* at 352. Justice Scalia, joined by Justice Thomas, expressed concern that this scheme would lead to "constitutional violations" if a defendant's sentence is "upheld as reasonable only because of the existence of judge-found facts." *Id.* at 374 (opinion concurring in part and concurring in the judgment). In response, the Court stated that that question was "not presented by this case." *Id.* at 353. Justice Stevens, joined by Justice Ginsburg, noted that "[s]uch a hypothetical case should be decided if and when it arises." *Id.* at 366 (concurring opinion).

Seven years later, Justice Scalia, joined by Justices Thomas and Ginsburg, noted the pressing need for the Court to resolve the question. See *Jones*, 135 S. Ct. at 8-9 (opinion dissenting from the denial of certiorari). Justice Scalia observed that, ever since the question was reserved in *Rita*, the courts of appeals had "uniformly taken our continuing silence" on the question as "suggest[ing] that the Constitution *does* permit otherwise unreasonable sentences supported by judicial factfinding, so long as they are within the statutory range." *Id.* at 9. Justice Scalia urged the Court to grant certiorari in an appropriate case in order to "put an end to the unbroken string of cases disregarding the Sixth Amendment—or to eliminate the Sixth Amendment difficulty by acknowledging that all sentences below the statutory maximum are substantively reasonable." *Ibid.*

Shortly after Justice Scalia's opinion in *Jones*, then-Judge Gorsuch similarly observed that "[i]t is far from certain whether the Constitution allows" a judge to increase a defendant's sentence within the statutorily authorized range "based on facts the judge finds without the aid of a jury or the defendant's consent." *United States* v. *Sabillon-Umana*, 772 F.3d 1328, 1331 (10th Cir. 2014) (citing *Jones*). Three years later, however, that question remains unanswered by the Court, despite intervening opportunities to address it.

2. As several members of the Court have now recognized, the lower courts will continue to authorize sentences that would be unreasonable but for judge-found facts until this Court intervenes. In the decision below, the court of appeals rejected petitioner's Sixth Amendment argument as having "no support in existing law." App., *infra*, 106a n.72. And other courts have declined to adopt similar arguments in the absence of clearer guidance from this Court, despite admitting that "there is room for debate." *United States* v. *Briggs*, 820 F.3d 917, 922 (8th Cir. 2016), cert. denied, 137 S. Ct. 617 (2017); *United States* v. *Cassius*, 777 F.3d 1093, 1099 n.4 (10th Cir.) (calling argument about judge-found sentencing facts "precluded by binding precedent" but citing *Jones*), cert. denied, 135 S. Ct. 2909 (2015); see also *United States* v. *Settles*, 530 F.3d 920, 923-924 (D.C. Cir. 2008) (noting that "we understand why defendants find it unfair for district courts to rely on acquitted conduct when imposing a sentence," but ultimately relying on "binding precedent" to affirm the sentence), cert. denied, 555 U.S. 1140 (2009).

Numerous judges in the lower courts have urged a different approach or specifically importuned this Court to provide guidance, noting the importance of the question and the attendant uncertainty surrounding sentencing practices while the question remains open. See, *e.g.*,

United States v. *White*, 551 F.3d 381, 390 (6th Cir. 2008) (en banc) (Merritt, J., dissenting) (taking the position on behalf of six judges that, when judge-found enhancements increase the Guidelines range such that the sentence would be unreasonable absent those facts, "those judge-found facts are necessary for the lawful imposition of the sentence, thus violating the Sixth Amendment right to a jury trial"), cert. denied, 556 U.S. 1215 (2009); *United States* v. *Bell*, 808 F.3d 926, 932 (D.C. Cir. 2015) (per curiam) (Millett, J., concurring in denial of rehearing en banc) (noting that "only the Supreme Court can resolve the contradictions in the current state of the law"), cert. denied, 137 S. Ct. 37 (2016); *id.* at 927 (Kavanaugh, J., concurring in denial of rehearing en banc) ("shar[ing] Judge Millett's overarching concern" and observing that a solution "would likely require" intervention by this Court).[2] The Court should accept the recurrent invitation to intervene and finally resolve the question presented.

B. The Decision Below Is Erroneous

The court of appeals erred when it concluded that petitioner's Sixth Amendment argument had "no support" in existing law. App., *infra*, 107a n.72. In so concluding, the court of appeals ignored the development of this Court's Sixth Amendment jurisprudence and the serious concerns raised by numerous members of this Court.

The Sixth Amendment was intended to preserve the "jury's historic role as a bulwark between the State and the accused at the trial for an alleged offense." *Southern*

---

[2] See also *United States* v. *Canania*, 532 F.3d 764, 776-778 (8th Cir.) (Bright, J., concurring), cert. denied, 555 U.S. 1037 (2008); *United States* v. *Mercado*, 474 F.3d 654, 663 (9th Cir. 2007) (Fletcher, J., dissenting), cert. denied, 552 U.S. 1297 (2008); *United States* v. *Faust*, 456 F.3d 1342, 1349 (11th Cir.) (Barkett, J., specially concurring), cert. denied, 549 U.S. 1046 (2006).

Union Co. v. *United States*, 567 U.S. 343, 350 (2012) (citation omitted). The Sixth Amendment's guarantee of a trial by jury is a constitutional protection "of surpassing importance," *Apprendi* v. *New Jersey*, 530 U.S. 466, 476-477 (2000), and it "has occupied a central position in our system of justice by safeguarding a person accused of a crime against the arbitrary exercise of power by prosecutor or judge," *Batson* v. *Kentucky*, 476 U.S. 79, 86 (1986).

As is relevant here, the jury trial right is a "fundamental reservation" of jury power that ensures that a judge's "authority to sentence derives *wholly* from the jury's verdict." *Blakely* v. *Washington*, 542 U.S. 296, 306 (2004) (emphasis added). In *Apprendi*, this Court held that "facts that increase the prescribed range of penalties to which a criminal defendant is exposed" must either be admitted by the defendant or submitted to a jury. 530 U.S. at 490; see *Blakely*, 542 U.S. at 303. The Court reaffirmed that principle in *Alleyne* v. *United States*, 133 S. Ct. 2151 (2013), explaining that, "[w]hen a finding of fact alters the legally prescribed punishment so as to aggravate it, the fact necessarily forms a constituent part of a new offense and must be submitted to the jury." *Id.* at 2162. Most recently, in *Hurst* v. *Florida*, 136 S. Ct. 616 (2016), the Court declared Florida's capital sentencing scheme unconstitutional under the Sixth Amendment because it permitted a judge, not a jury, to find the aggravating circumstances necessary to support a defendant's sentence. *Id.* at 624.

The foregoing principles apply with equal force where, as here, judicial factfinding alters the Guidelines range and thereby encourages the court to impose a sentence that would otherwise be substantively unreasonable. Although the Sentencing Guidelines are no longer mandatory, they "remain the starting point for every sentencing calculation in the federal system." *Peugh* v. *United*

States, 133 S. Ct. 2072, 2083 (2013). "[I]f the judge uses the sentencing range as the beginning point" for the sentencing decision, "*then the Guidelines are in a real sense the basis for the sentence*," even if the ultimate sentence deviates from the Guidelines range. *Ibid.* (citation omitted). A sentencing court is not free to impose a sentence, even if it falls within the statutory range, without taking account of the Guidelines range and explaining any variance. To do otherwise constitutes procedural error and results in an unlawful sentence. See *ibid.*

In the absence of a decision by this Court squarely addressing the question presented, however, the Sixth Amendment right to trial by jury is being "lost * * * by erosion." *Apprendi*, 530 U.S. at 483 (citation omitted). The government is now frequently permitted a "second bite at the apple" at sentencing when it presents a judge with conduct for which the defendant was acquitted or (as here) not even charged. That strategy—whereby the government relies on facts the jury either refused or had no opportunity to find—"entirely trivializes" the jury's "principal fact-finding function." *Canania*, 532 F.3d at 776 (Bright, J., concurring).

Even within the statutory range, there are sentences that would be unlawful but for a judge's factfinding. Under this Court's Sixth Amendment precedents, facts that justify an otherwise unreasonable sentence must be found by a jury or admitted by the defendant before they can be used to increase the defendant's sentence. This Court should grant review and definitively hold that the practice of sustaining an otherwise unreasonable sentence through judicial factfinding is unconstitutional.

C. The Question Presented Warrants Review In This Case

This case is a particularly egregious example of judicial factfinding. Petitioner was convicted by the jury of distributing "one kilogram or more" of heroin, "five kilograms or more" of cocaine, "ten grams or more" of LSD, and "500 grams or more" of methamphetamine. D. Ct. Dkt. 183, at 1-3 (Feb. 5, 2015) (verdict form). Petitioner was not charged with, and the jury was never asked to render a verdict on, the alleged commissioning of murders connected to the Silk Road.

At sentencing, however, the district court made a number of factual findings—most significantly, that petitioner commissioned five murders and distributed a total quantity of drugs far in excess of that found by the jury. Those factual findings greatly increased petitioner's Guidelines range. C.A. App. 1462-1470; App., *infra*, 26a-27a. The judge also made findings that six drug deaths were "in some way" related to the Silk Road, although those deaths similarly were not charged in the indictment or part of the jury's verdict. C.A. App. 1472. In all, the district court's factual findings resulted in enhancements that raised petitioner's Guidelines sentencing range from a determinate range of no more than thirty years to a "range" of life imprisonment. App., *infra*, 26a-27a.

The court of appeals acknowledged as much: it confirmed that petitioner's "high offense level" under the Guidelines "largely resulted" from the district court's findings about the "quantity of drugs trafficked using Silk Road" as well as the enhancement for "directing the use of violence." App., *infra*, 26a-27a. Although the court of appeals stated that "a life sentence for selling drugs alone would give us pause," it ultimately found petitioner's life sentence substantively reasonable because of the district court's findings. *Id.* at 100a-101a & n.68.

Absent those findings, petitioner's sentence of life imprisonment would plainly have been substantively unreasonable. As the Sentencing Commission has recognized, "[t]he drug trafficking guidelines specifically provide for a sentence of life imprisonment * * * only where death or serious bodily injury resulted from the use of the drug" and the defendant has prior convictions. United States Sentencing Commission, *Life Sentences in the Federal System* 3 (Feb. 2015) (footnote omitted) <tinyurl.com/ussclife>. In cases involving "very large" quantities of drugs and significant prior criminal history, "the sentencing range can include life imprisonment * * * only as the sanction at the top of the range." *Ibid.* Here, however, petitioner is a young first-time offender who was never charged with causing any death or bodily injury. This case directly implicates the question presented, and it does so in the most acute of circumstances: a high-profile criminal prosecution that heaped intense scrutiny and pressure on the sentencing judge, resulting in a sentence of life imprisonment without parole for a first-time offender.

In this case, the sentencing judge's factual findings elevated the Guidelines range from a determinate range of no more than thirty years to a "range" of life imprisonment, "condemn[ing] a young man to die in prison." App., *infra*, 108a. The unconstitutional practice of judicial fact-finding "has gone on long enough." *Jones*, 135 S. Ct. at 9 (Scalia, J., dissenting from the denial of certiorari). The Court should grant certiorari on that question, as well as the Fourth Amendment question, and review this consequential conviction and sentence on the merits.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

KANNON K. SHANMUGAM
ALLISON JONES RUSHING
MASHA G. HANSFORD
MICHAEL J. MESTITZ
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
(202) 434-5000
kshanmugam@wc.com

DECEMBER 2017